IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) A computer program product for controlling a computer to scan computer files for malware, said computer program product comprising:

malware scanning code operable to malware scan all computer files stored within a storage location as addressed by an operating system to identify any computer files stored within said storage location that contain malware;

identification code operable if no computer files containing malware are found in said storage location, to identify said storage location as a clean storage location; and

when subsequently reading a computer file, determination code operable to determine whether or not said computer file is stored within a clean storage location and:

if said computer file is stored within a clean storage location, then permitting reading of said computer file without further malware scanning; and

if said computer file is not stored within a clean storage location, then malware scanning said computer file;

wherein said malware scanning of all computer files stored within a storage location is performed as a background task that occurs as a function of when an associated computer system is at least substantially idle;

wherein said malware scanning of all computer files stored within a storage location as a background task is performed with more thorough scanning options selected than for on-access scanning applied to computer files not stored within clean storage locations and being accessed by a user.

2. (Original) A computer program product as claimed in claim 1, wherein said malware scanning of all computer files stored within a storage location is performed upon a set of user specified storage locations from within all storage locations accessible to a user.

3. (Cancelled)

4. (Cancelled)

5. (Original) A computer program product as claimed in claim 1, wherein a computer file is malware scanned before being written to a clean storage location.

6. (Original) A computer program product as claimed in claim 1, wherein said malware scanning code uses malware definition data to identify malware and, upon updating of said malware definition data to give updated malware definition data, said storage location is no longer identified as a clean storage area until it has been malware scanned using said updated malware definition data and no computer files containing malware are found in said storage location.

7. (Original) A computer program product as claimed in claim 6, wherein, when said storage area is being malware scanned with said updated malware definition data, computer files written to said storage location after said storage location was previously identified as a clean storage location are malware scanned before computer files that are unaltered since said storage location was previously identified as a clean storage location.

8. (Original) A computer program product as claimed in claim 1, wherein said malware is one or more of a computer virus, a worm, a Trojan, a banned computer file, a banned word and a banned image.

9. (Currently Amended) A method of scanning computer files for malware, said method comprising the steps of:

malware scanning all computer files stored within a storage location as addressed by an operating system to identify any computer files stored within said storage location that contain malware;

if no computer files containing malware are found in said storage location, then identifying said storage location as a clean storage location; and

when subsequently reading a computer file, determining whether or not said computer file is stored within a clean storage location, whereupon:

if said computer file is stored within a clean storage location, then permitting reading of said computer file without further malware scanning; and

if said computer file is not stored within a clean storage location, then malware scanning said computer file;

wherein said step of malware scanning all computer files stored within a storage location is performed as a background task that occurs as a function of when an associated computer system is at least substantially idle;

wherein said step of malware scanning all computer files stored within a storage location as a background task is performed with more thorough scanning options selected than for on-access scanning applied to computer files not stored within clean storage locations and being accessed by a user.

10. (Original) A method as claimed in claim 9, wherein said step of malware scanning all computer files stored within a storage location is performed upon a set of user specified storage locations from within all storage locations accessible to a user.

11. (Cancelled)

12. (Cancelled)

13. (Original) A method as claimed in claim 9, wherein a computer file is malware scanned before being written to a clean storage location.

14. (Original) A method as claimed in claim 9, wherein said malware scanning uses malware definition data to identify malware and, upon updating of said malware definition data to give updated malware definition data, said storage location is no longer identified as a clean storage area until it has been malware scanned using said updated malware definition data and no computer files containing malware are found in said storage location.

15. (Original) A method as claimed in claim 14, wherein, when said storage area is being malware scanned with said updated malware definition data, computer files written to said storage location after said storage location was previously identified as a clean storage location are malware scanned before computer files that are unaltered since said storage location was previously identified as a clean storage location.

16. (Original) A method as claimed in claim 9, wherein said malware is one or more of a computer virus, a worm, a Trojan, a banned computer file, a banned word and a banned image.

17. (Currently Amended) Apparatus for scanning computer files for malware, said apparatus comprising:

malware scanning logic operable to malware scan all computer files stored within a storage location as addressed by an operating system to identify any computer files stored within said storage location that contain malware;

identification logic operable if no computer files containing malware are found in said storage location, to identify said storage location as a clean storage location; and

when subsequently reading a computer file, determination logic operable to determine whether or not said computer file is stored within a clean storage location and:

if said computer file is stored within a clean storage location, then permitting reading of said computer file without further malware scanning; and

if said computer file is not stored within a clean storage location, then malware scanning said computer file;

wherein said malware scanning of all computer files stored within a storage location is performed as a background task that occurs as a function of when an associated computer system is at least substantially idle;

wherein said malware scanning of all computer files stored within a storage location as a background task is performed with more thorough scanning options selected than for on-access scanning applied to computer files not stored within clean storage locations and being accessed by a user.

18. (Previously Presented) Apparatus as claimed in claim 17, wherein said malware scanning of all computer files stored within a storage location is performed upon a set of user specified storage locations from within all storage locations accessible to a user.

19. (Cancelled)

20. (Cancelled)

21. (Previously Presented) Apparatus as claimed in claim 17, wherein a computer file is malware scanned before being written to a clean storage location.

22. (Previously Presented) Apparatus as claimed in claim 17, wherein said malware scanning logic uses malware definition data to identify malware and, upon updating of said malware definition data to give updated malware definition data, said storage location is no longer identified as a clean storage area until it has been malware scanned using said updated malware definition data and no computer files containing malware are found in said storage location.

23. (Previously Presented) Apparatus as claimed in claim 22, wherein, when said storage area is being malware scanned with said updated malware definition data, computer files written to said storage location after said storage location was previously identified as a clean storage location are malware scanned before computer files that are unaltered since said storage location was previously identified as a clean storage location.

24. (Original) Apparatus as claimed in claim 17, wherein said malware is one or more of a computer virus, a worm, a Trojan, a banned computer file, a banned word and a banned image.

25. (Previously Presented) A computer program product as claimed in claim 1, wherein, if said computer file is stored within said clean storage location, then said

computer file is permitted to be read without further time spent on malware-related processing.

26. (Previously Presented) A computer program product as claimed in claim 6, wherein said malware scanning using said updated malware definition data is performed as another background task.

27. (Previously Presented) A computer program product as claimed in claim 1, wherein all of said computer files stored within said storage location addressed by said operating system share a common logical storage location as viewed by said operating system such that said logical storage location includes computer files sharing similar characteristics.

28. (New) A computer program product as claimed in claim 1, wherein the background task avoids interference with a responsiveness of the computer system when the user starts to use the computer system.